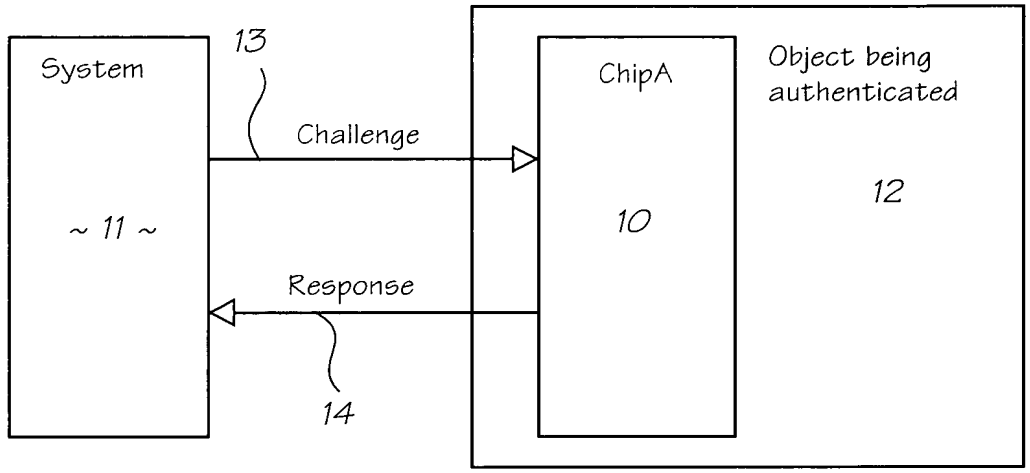

System
13
Challenge
~ 11 ~
Response
14
ChipA
10
Object being
authenticated
12

FIG. 1

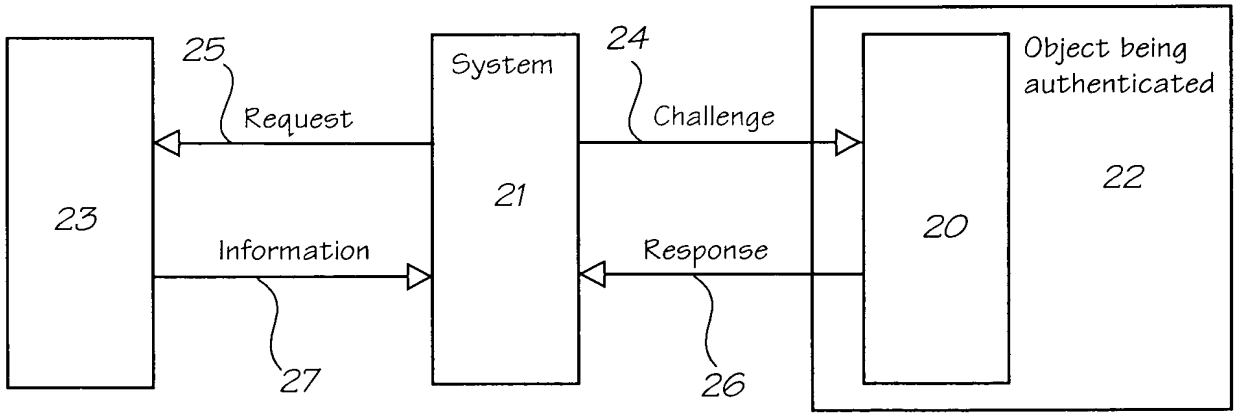

25
Request
23
Information
27
System
21
24
Challenge
Response
26
20
Object being
authenticated
22

FIG. 2

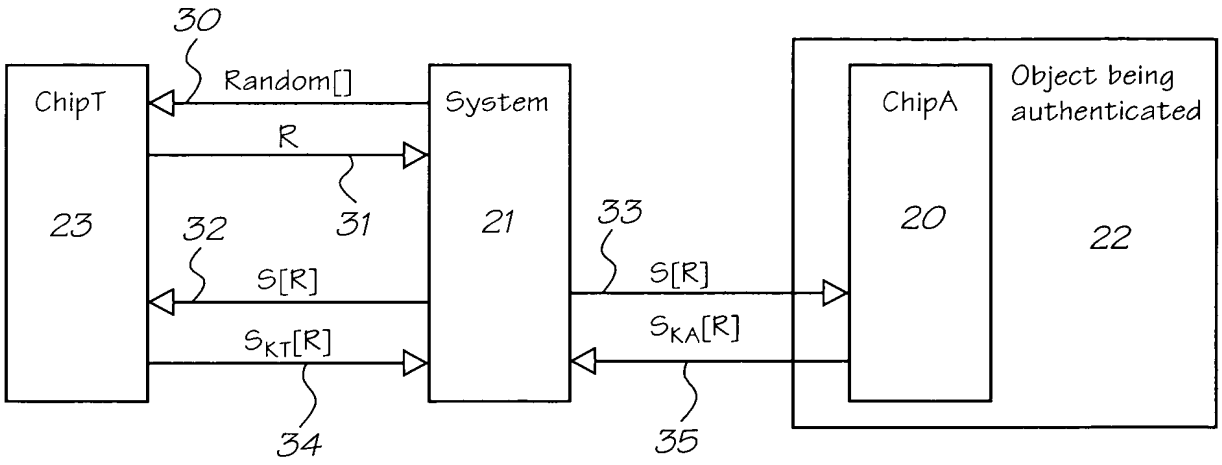

30
ChipT
Random[]
System
ChipA
Object being authenticated
R
23
31
21
20
22
32
33
S[R]
S[R]
$S_{KA}[R]$
$S_{KT}[R]$
34
35

FIG. 3

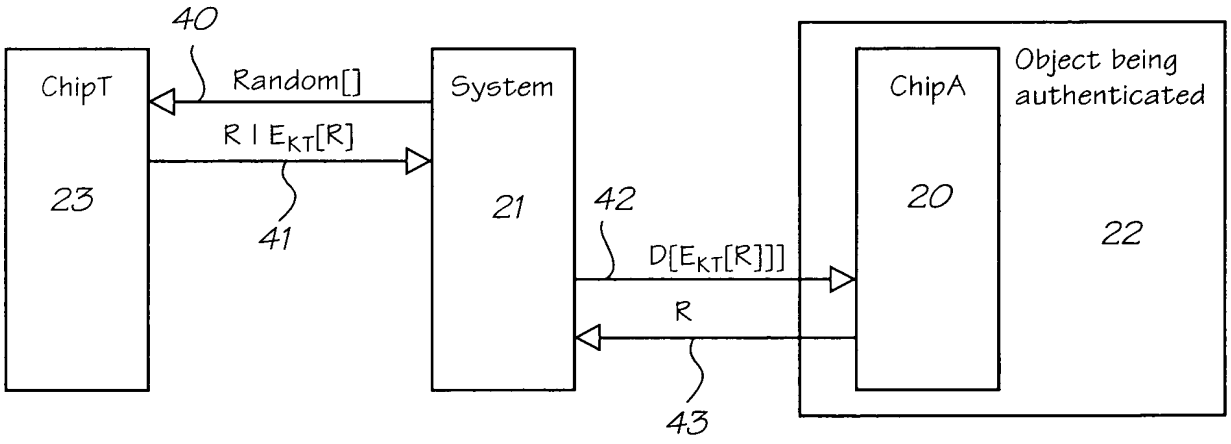

40
ChipT
Random[]
System
ChipA
Object being authenticated
R | $E_{KT}[R]$
23
41
21
20
22
42
$D[E_{KT}[R]]]$
R
43

FIG. 4

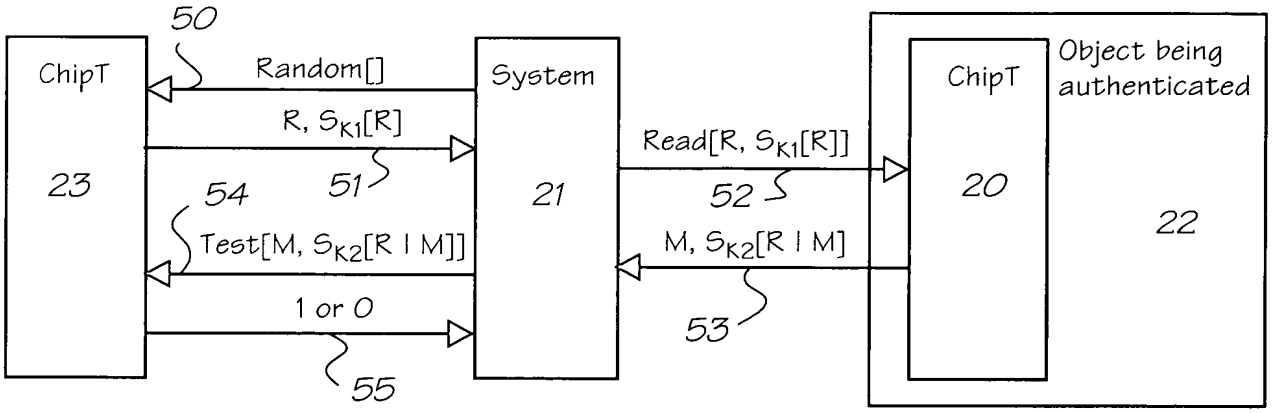

50
ChipT
23
Random[]
R, S_{K1}[R]
51
54
Test[M, S_{K2}[R | M]]
1 or 0
55
System
21
Read[R, S_{K1}[R]]
52
M, S_{K2}[R | M]
53
ChipT
20
Object being authenticated
22

FIG. 5

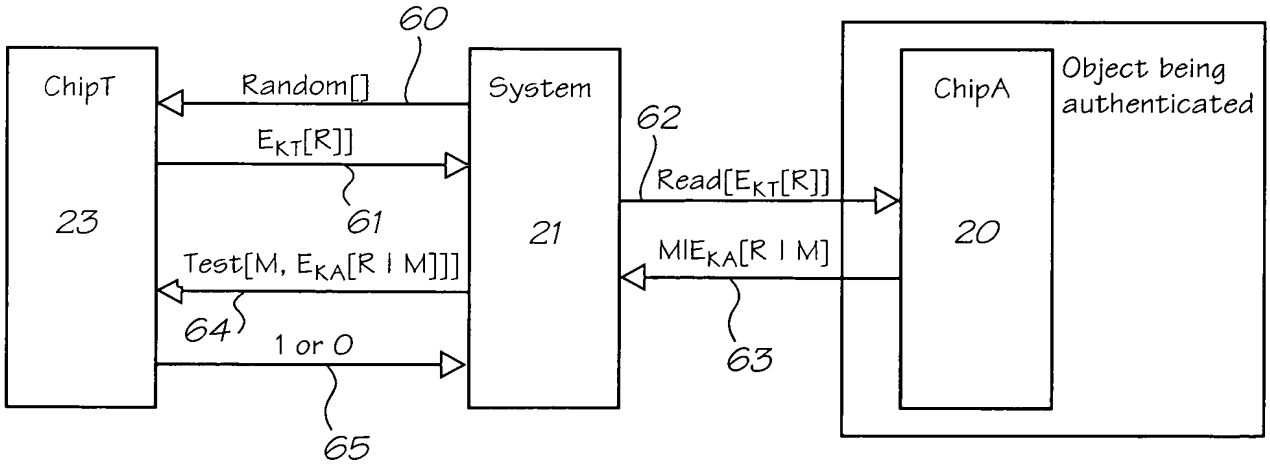

60
ChipT
23
Random[]
E_{KT}[R]]
61
Test[M, E_{KA}[R | M]]]
64
1 or 0
65
System
21
62
Read[E_{KT}[R]]
M|E_{KA}[R | M]
63
ChipA
20
Object being authenticated

FIG. 6

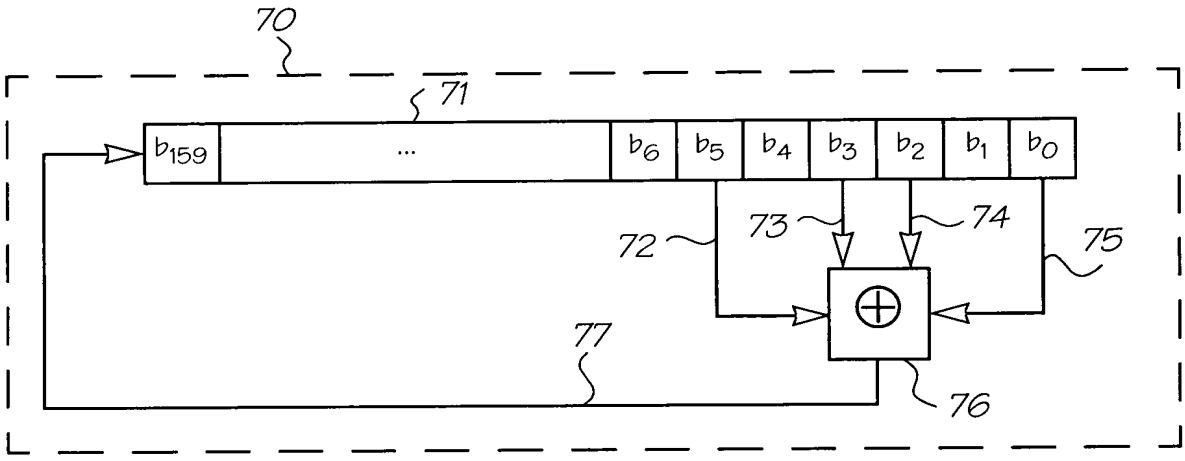


FIG. 7

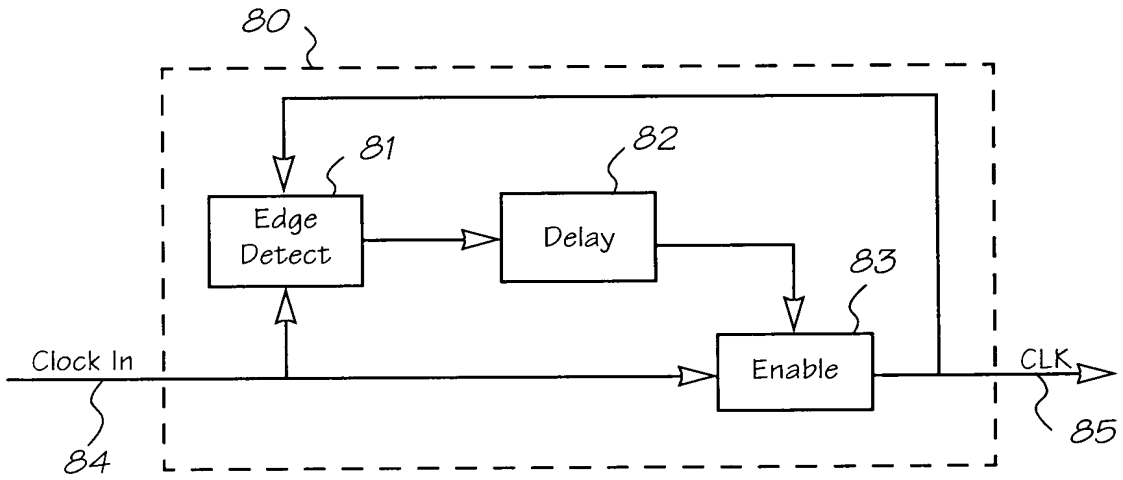


FIG. 8

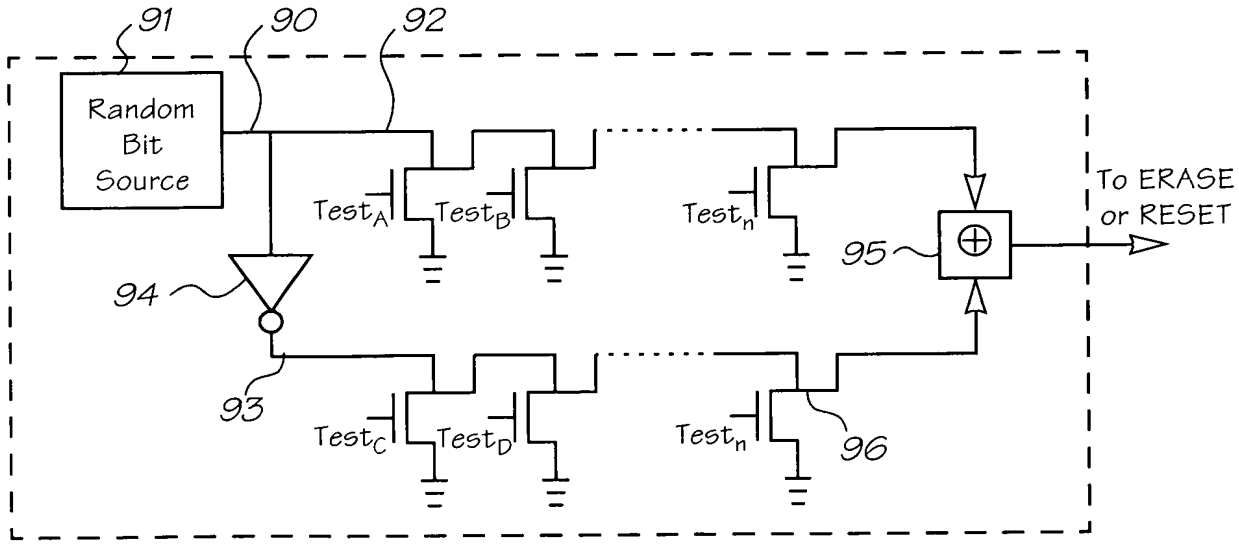


FIG. 9

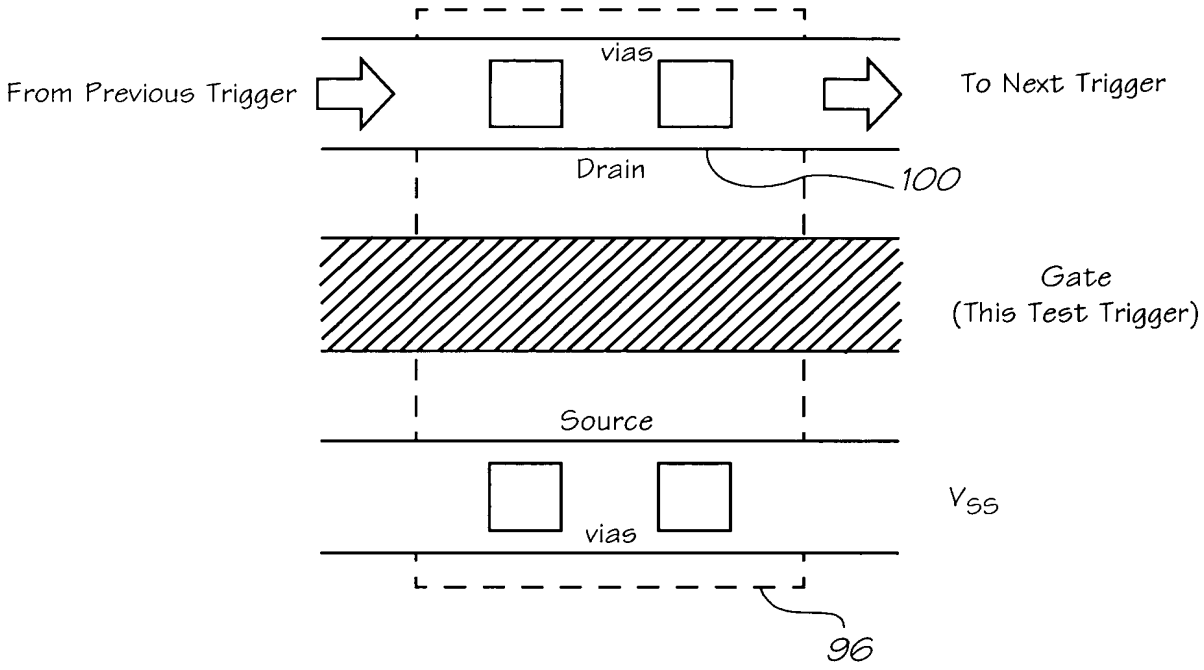

From Previous Trigger
vias
To Next Trigger
Drain
100
Gate
(This Test Trigger)
Source
V_{SS}
vias
96

FIG. 10

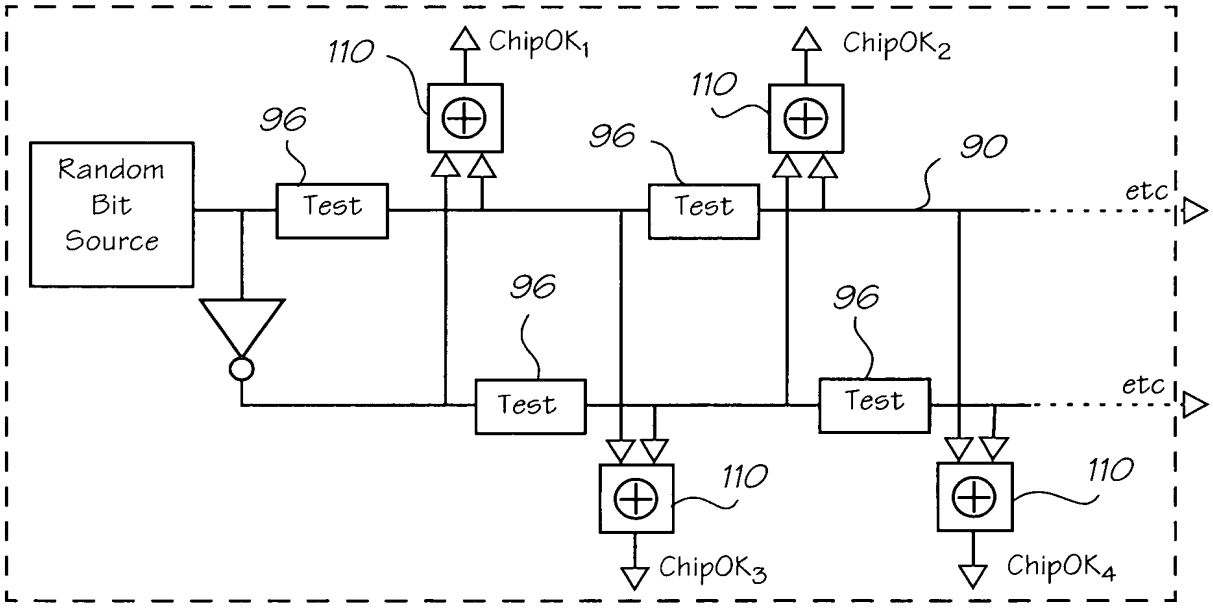

Random Bit Source
Test
Test
Test
Test
110
110
110
110
96
96
96
96
90
ChipOK1
ChipOK2
ChipOK3
ChipOK4
etc
etc

FIG. 11

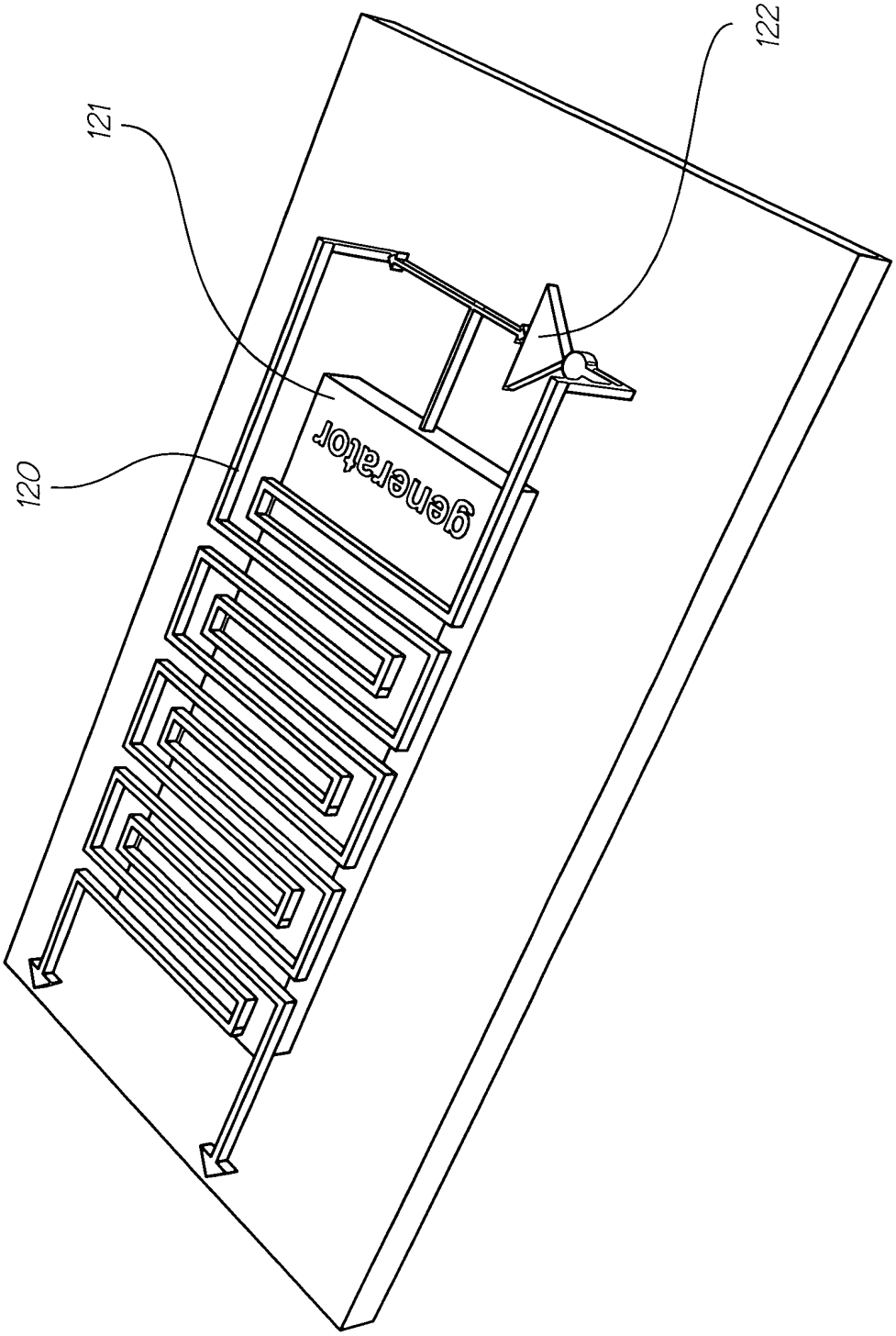


FIG. 12

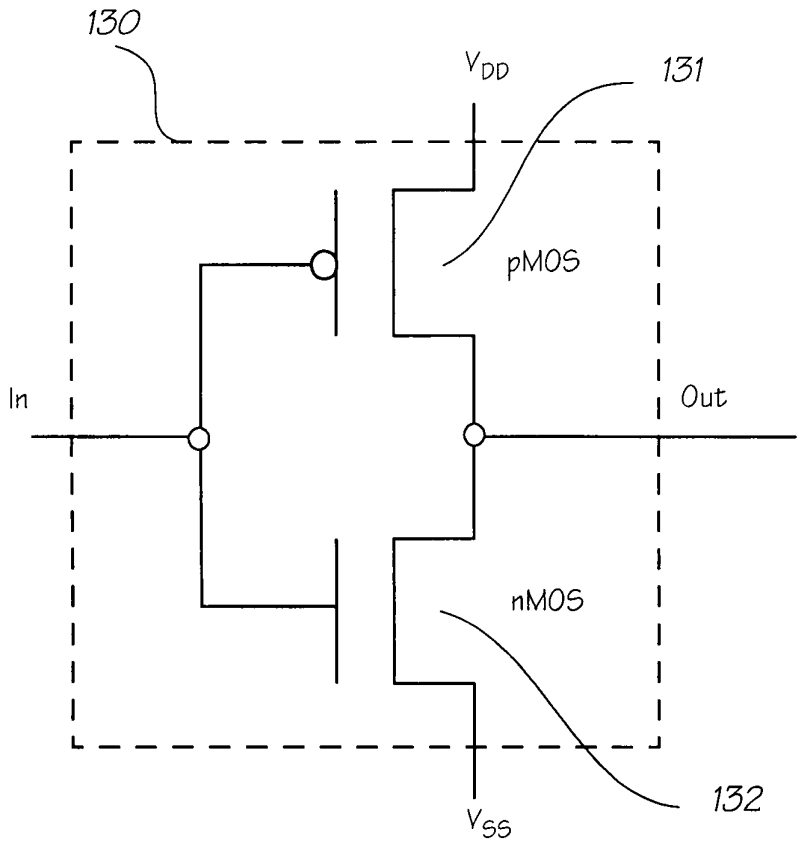

130
V_{DD}
131
pMOS
In
Out
nMOS
V_{SS}
132

FIG. 13

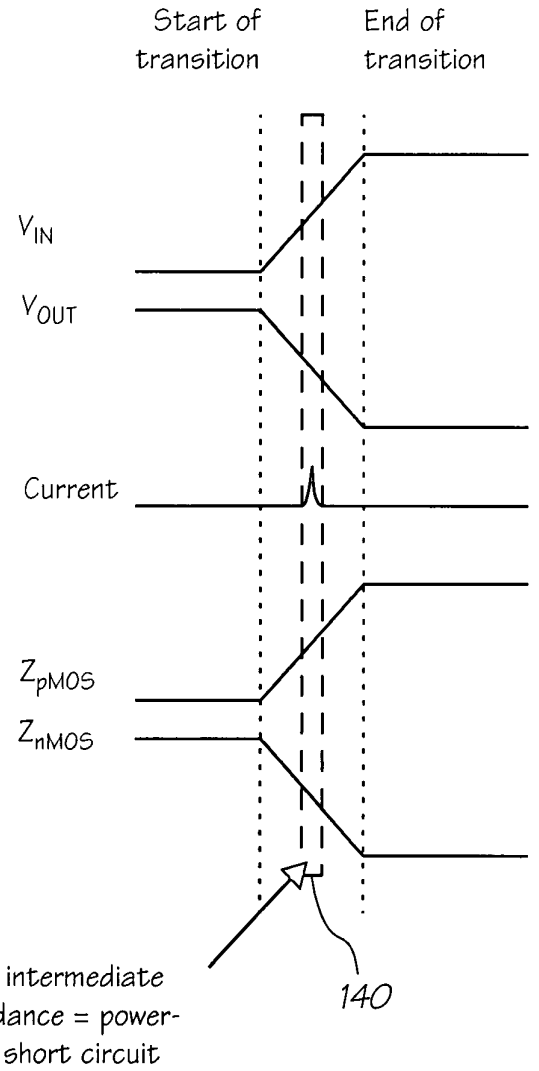

Start of transition
End of transition
V_{IN}
V_{OUT}
Current
Z_{pMOS}
Z_{nMOS}
Both intermediate impedance = power-GND short circuit
140

FIG. 14

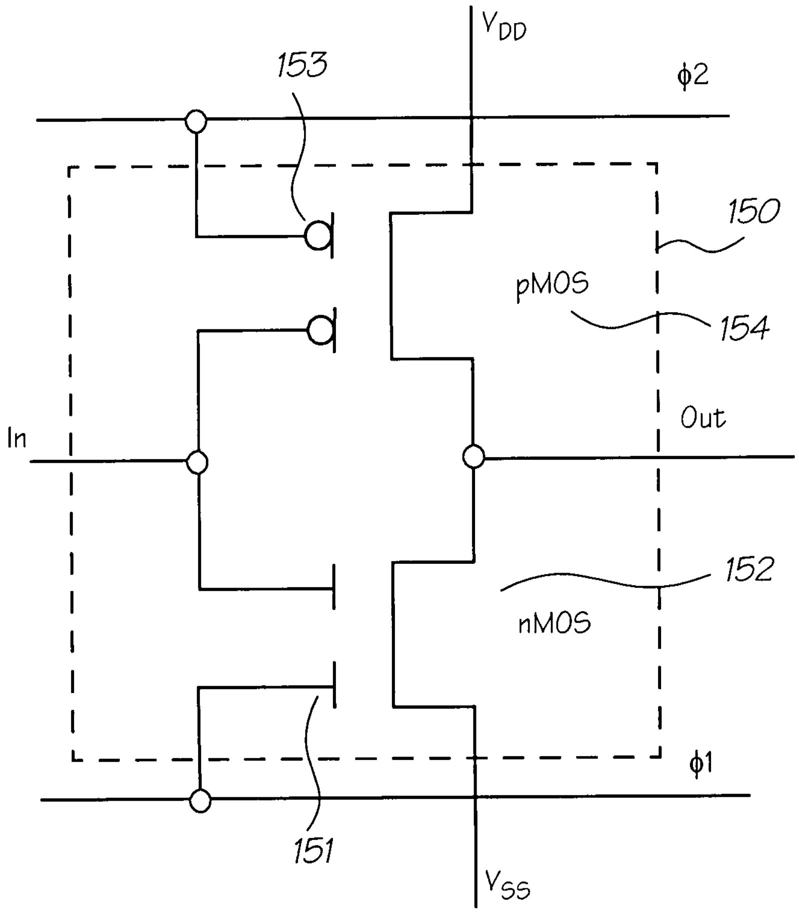
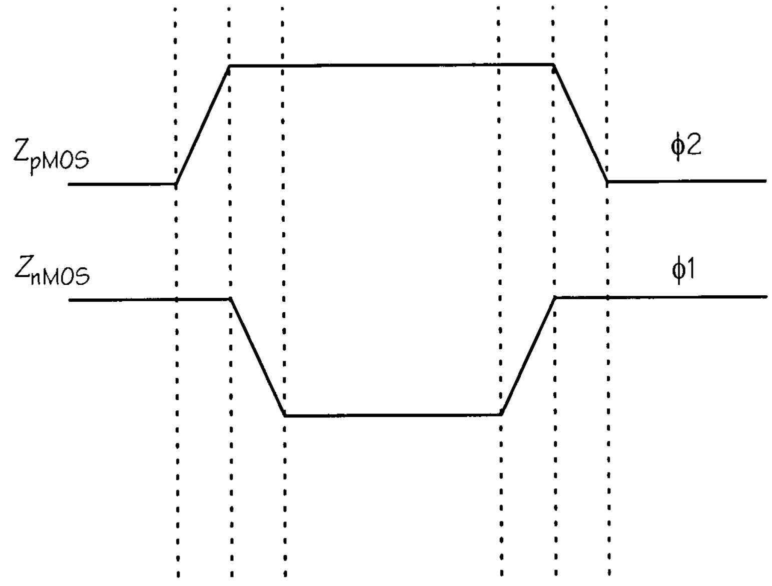


FIG. 15



Non-overlapping clocks

FIG. 16